

# Beschermen tegen CSCwi63113 tijdens upgrade naar 7.2.6

## Inhoud

---

[Inleiding](#)

[Achtergrond](#)

[SNMP uitschakelen voor de upgrade](#)

[FMC Stappen:](#)

[Stap 1: Meld u aan bij uw VCC](#)

[Stap 2: Navigeren naar apparaten > Platform-instellingen](#)

[Stap 3: Bewerk het beleid dat gekoppeld is aan uw FTD-apparaten](#)

[Stap 4: Selecteer SNMP](#)

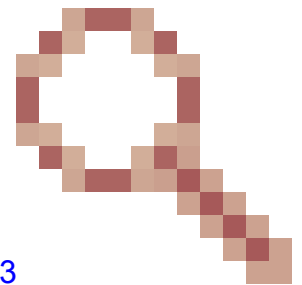
[Stap 5: SNMP-servers uitschakelen](#)

[Stap 6: Opslaan naar beleid en implementeren](#)

[Wat te doen Als u al geupgrade hebt en een bootloop ervaren:](#)

---

## Inleiding



Dit document beschrijft informatie met betrekking tot Cisco bug-id [CSCwi63113](#) en hoe u problemen kunt voorkomen tijdens de upgrade naar FTD versie 7.2.6.

## Achtergrond

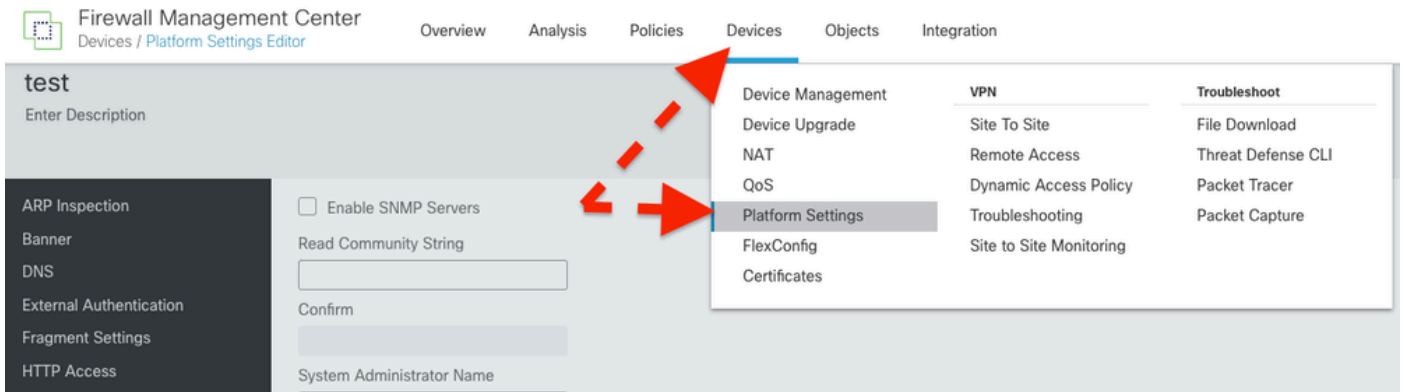
Cisco Firepower Threat Defence softwareversie 7.2.6 bevat Cisco bug-id [CSC63113](#), die verhindert dat sommige apparaten worden opgestart wanneer SNMP is ingeschakeld. Voordat u 7.2.6 installeert, moet u SNMP uitschakelen totdat u kunt upgraden naar 7.2.7 of hoger. Er wordt gewerkt aan een oplossing hiervoor, die uiterlijk 3 mei 2024 zal worden vrijgegeven als 7.2.7. Bovendien zal Cisco 7.2.5.2 vóór 6 mei 2024 uitbrengen, hetgeen 7.2.5.1 is met alleen de oplossingen voor CVE-2024-20353, CVE-2024-20359 en CVE-2024-20358.

## SNMP uitschakelen voor de upgrade

FMC Stappen:

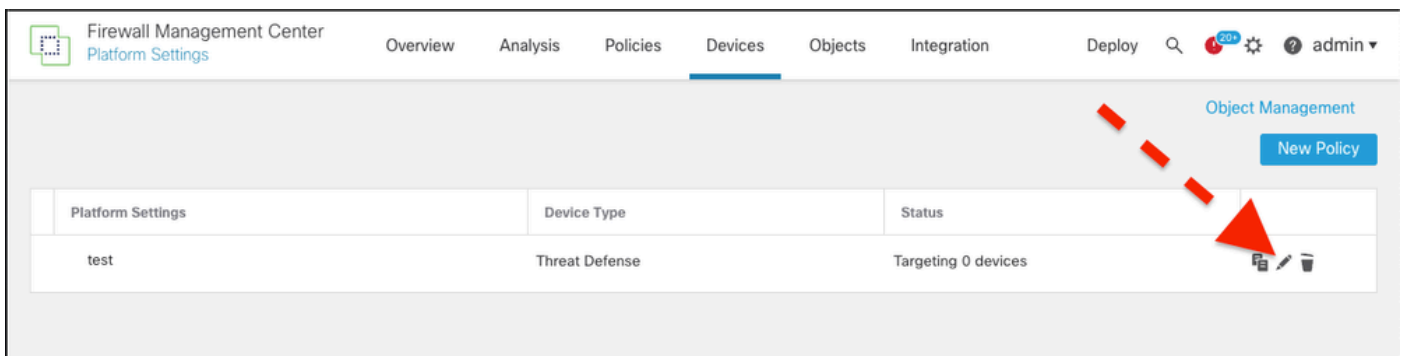
Stap 1: Meld u aan bij uw VCC

## Stap 2: Navigeren naar apparaten > Platform-instellingen



The screenshot shows the Firewall Management Center interface. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Devices' tab is active. On the left, a sidebar lists various settings categories: ARP Inspection, Banner, DNS, External Authentication, Fragment Settings, and HTTP Access. The main content area is titled 'test' and contains a form with fields for 'Enable SNMP Servers', 'Read Community String', 'Confirm', and 'System Administrator Name'. A dropdown menu is open over the 'Devices' tab, listing options such as Device Management, Device Upgrade, NAT, QoS, Platform Settings (highlighted), FlexConfig, Certificates, VPN, Site To Site, Remote Access, Dynamic Access Policy, Troubleshooting, Site to Site Monitoring, and Troubleshoot (with sub-items: File Download, Threat Defense CLI, Packet Tracer, Packet Capture). Red dashed arrows indicate the navigation path from the 'Devices' tab to the 'Platform Settings' option in the dropdown menu.

## Stap 3: Bewerk het beleid dat gekoppeld is aan uw FTD-apparaten



The screenshot shows the Firewall Management Center interface with the 'Platform Settings' overview table. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, Integration, Deploy, a search icon, a gear icon, and a user profile 'admin'. The 'Devices' tab is active. On the right, there is an 'Object Management' section with a 'New Policy' button. The main content area is a table with the following data:

Platform Settings	Device Type	Status	
test	Threat Defense	Targeting 0 devices	

Red dashed arrows point from the 'Object Management' section towards the action icons in the table row.

## Stap 4: Selecteer SNMP



# test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

Hosts

Users

SNMP Traps

Interface	Network	SNMP Version	Poll/Trap
Management	backup_c1	1	Poll,Trap

Stap 5: SNMP-servers uitschakelen



test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

Stap 6: Opslaan naar beleid en implementeren

Firewall Management Center  
Platform Settings Editor

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin ▾

test  
Enter Description

ARP Inspection  
Banner  
DNS  
External Authentication  
Fragment Settings  
HTTP Access  
ICMP Access  
SSH Access  
SMTP Server

Enable SNMP Servers  
Read Community String  
Confirm  
System Administrator Name  
Location

vFTD | Ready for Deployment

Advanced Deploy Deploy All

1 device is available for deployment

Bekijk het defect voor meer actuele informatie: Cisco bug ID [CSC63113](#).

Als u verdere informatie nodig hebt, neem dan contact op met Cisco TAC ([support.cisco.com](https://support.cisco.com)) en reference Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

**Wat te doen Als u al geupgrade hebt en een bootloop ervaren:**

Als u al bent bijgewerkt naar 7.2.6 en geconfronteerd wordt met de effecten van Cisco bug-id [CSCwi63113](#), neem dan contact op met Cisco TAC ([support.cisco.com](https://support.cisco.com)).

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.